Spirent CF20

适用于CyberFlood 应用和安全测试解决方案

适用于CyberFlood解决方案的CF20可作为1G、10G、40G和100G接口的高级测试选项。

CF20可测试网络基础设施和Web应用基础设施的有效性和性能，对您的安全态势、服务质量(QoS)和体验质量(QoE)进行验证。CF20充分利用了CyberFlood的强大能力，将多种测试功能合并到小型独立设备中，为您提供更高的使用便利性。

应用

- 利用真实的攻击和入侵验证安全有效性
- 测试DDoS消减服务和下一代防火墙
- 创建极端的HTTPS流量负载，对加密容量和性能进行验证
- 利用不断更新的数据库来生成各类应用负载流量，其中包含超过9000种应用场景和应用流，能够对应用ID策略和性能执行全面验证
- 利用当日和最新恶意软件样例执行测试
- 回放大规模的定制流量
- 先进的模糊攻击测试可创建出数以百万计的测试场景，迅速、高效地发现未知的漏洞

在今天要求极为苛刻的商业环境中，理解网络安全的有效性和性能至关重要，而且今天的用户需要的是非常高的访问和防故障安全性。有了思博伦的CF20 CyberFlood测试平台，我们就可以比以往任何时候都更方便地通过前瞻的方式测试内容感知网络和安全基础设施。它的多速率可以实现众多的测试用例，并且涵盖目前在用网络接口中的绝大多数，同时还可提供适用于企业、数据中心和服务商的众多1G至100G选项。CF20是一种完全自给自足的解决方案，具备基于Web的内建控制器，可管理各类测试例和资产，并且标配了先进的加密加速技术，能够在大规模条件下创建出数量巨大的深层HTTPS流量。

凭借 CyberFlood 实现的用户真实性

CyberFlood使用TestCloud™来访问数以千计的应用，这样您就可以生成包含可靠有效负载的流量，实现真实的安全、性能负载和功能测试。CyberFlood可以使用Spirent TestCloud的最新应用来创建测试，同时还能为用户提供自行导入应用的能力，从而重现出大规模条件下的定制应用。

利用最新的攻击及其变体快速开展测试，包括Wannacry、Petya、Crisis、Nemucod、Spora和Cerber等。CyberFlood可以让您访问最新的数据库，其中包含数千种攻击、实时恶意软件配置和向量等，因此您可以对大规模攻击和应用的任意组合进行测试。迅速、简便地确定安全策略如何防范各类攻击，同时还可允许合法的用户流量尽可能不受阻碍地顺利通过。利用大规模批量和协议DDoS进行测试，验证您的消减策略是否发挥了应有的作用。

利用先进的模糊攻击技术找出未知的漏洞

CyberFlood广泛的扩展能力、性能和安全测试解决方案可以提供先进的模糊攻击选项，实现TLS v1.3等70余种常用和现行协议上近乎无限数量的模糊测试例。先进模糊攻击选项让您能够将某个端点当作目标，或对线内系统进行测试，找出其中可能存在的弱点、和漏洞。

特性和优势

- **易用性——**极其易于使用且非常直观的图形用户界面，可以帮助用户立即对复杂的配置完成设置。从利用世界视角的地图设置全球IP，到对各类协议进行播放，CyberFlood都可以让安全和性能测试变得更加容易。由于具备简便的拆箱即用设置，CF20还可大幅降低部署和管理的复杂程度。
- **经济性——**以高性价比获得具备正确特性、性能和能力的强大CyberFlood解决方案，而在性能方面却毫不妥协。此外，由于机架空间、供电和散热的要求更低，还能有效地降低您的总体拥有成本。
- **网络安全性测试——**为安全的网络通信和漏洞评估提供广泛的测试，以及不断扩大和更新的数据库，内含超过3000种攻击配置和17000种恶意软件样例。
  - 对网络安全设备的能力进行验证，探测和消减数千种已知和当日攻击。
  - 利用CyberFlood的模糊攻击，可对网络设备和已部署协议的弹性进行测试，验证其应对数百万种意外和恶意输入的能力。
  - 测试网络设备的检查恶意软件、受感染主机、无用URL和垃圾邮件，以及采取恰当行动的能力。
- **应用——**用户可以利用CyberFlood快速、简便地对最新和最常用的应用与攻击(持续更新)进行测试，所有这一切都可实现无与伦比的真实度和扩展性。用户可以将其解决方案推向极限，同时确保基础设施能够承受真实的需求。
- **强大的能力和性能——**准确的性能和规模:CF20可提供准确的性能配置，能够有效地对网络施加考验，找出最大用户连接、应用流量吞吐能力，以及安全的有效性。
- **内建的密文加速——**CF20标配内建的密文加速技术，可以大幅提高加密流量的速度和带宽，包括各类强大的常用加密类型。
- **跨平台兼容性——**CF20具备与其它CyberFlood平台的兼容性，使用户拥有了在多种可用平台上使用CyberFlood测试的最大灵活性。

Spirent CF20

适用于CyberFlood

技术规格			
可用硬件配置			
带2xQSFP28接口的CF20，适用于10G/40G/100G运行	• 8x10G扇出 • 2x40G	• 2x100G • 不包含收发器	• 密文加速模块
带2x SFP28和4x10G/1G接口的CF20 ——即将推出	• 4x10G/1G SFP+ • 8x10G扇出	• 2x40G • 2x100G	• 密文加速模块 • 不包含收发器
带8x10G/8x1G接口的CF20——即将推出	• 8x10G/1G SFP+	• 密文加速模块	• 不包含收发器
通过未来的授权选项，带2xQSFP28接口的CF20将具备25G和50G传输能力。			
软件授权选项			
性能测试软件	包含HTTP/HTTPs带宽、连接性和速率测试、先进混合流量测试、定制流量回放和DNS。		
安全和性能测试软件	包含所有CyberFlood选项，涵盖恶意软件和攻击下的网络安全评估、DDoS测试和所有性能测试软件选项。		
TestCloud订用	可针对应用场景、攻击/漏洞和恶意软件，提供永远更新的可下载内容的选项。		
先进模糊攻击	CyberFlood所提供的强大模糊攻击选项适用于超过70种独立的协议。		
CyberFlood特性详情			
基于Web的界面	易于使用的基于Web的多用户界面可以让综合性测试的设计和执行过程变得更加快速、简便和连贯。		
应用场景	超过9000种在用和常用应用及用户场景。		
攻击和漏洞	超过3000种攻击和漏洞，涵盖SQL注入、跨站点脚本、目标操作系统、在线设备、端点服务等领域。		
恶意软件	超过17000种最新和当日恶意软件样例，包括命令和控制行为，以及二进制、恶意软件转移场景。		
DDoS	测试时可使用不同的DDoS攻击来确认安全消减策略探测和阻止此类攻击的能力，且批量和协议DDoS攻击套装可配置独立的攻击测试，或与普通用户流量进行混合，以验证其对性能造成的影响。		
HTTPS/TLS测试	支持SSLv3、TLS v1.0、TLS v1.2和TLS v1.3，并提供可选择的证书和加密套装。		
CyberSecurity评估	迅速创建各类测试，在具备和不具备用户流量负载的情况下，对IDS、IPS NGFW和其它安全解决方案的有效性进行验证。		
HTTP连接测试	每秒打开数千至数百万个新的连接，确保您的被测设备能够应对网络中新的连接速率。		
HTTP带宽测试	使用仿真、真实的HTTP客户端和HTTP服务器，并利用可配置的网络拓扑结构，找出可实现的最大吞吐量。		
HTTP开放连接测试	在您被测设备的状态表中打开数百万个并发TCP连接，找出它所能支持的最大并行水平。同时还可利用HTTP协议来提高测试过程中的真实性。		
混合流量测试	利用真实的内建应用或TestCloud的扩充应用来测试应用性能所受的影响。可独立测量测试中添加的每种应用的带宽和成功率，确认被测网络所受的影响。		
流量回放	在大规模条件下回放您自己的流量配置，确定您在网络设备和服务上的客户流量流所受的影响。		
DNS测试	发送每秒数十万个需要由被测设备加以处理和传输的DNS检索，以及被测设备在DNS响应时需要处理的对应事件，从而对您的被测设备施加过度负载测试。		
模糊攻击测试	先进的模糊攻击测试，适用于对端点、直通和服务器端执行模糊攻击测试，并且具备全面的监视项目，可验证测试的健康程度和设备重启控制是否能够将系统带回已知状态，同时还可支持70余种常用的协议。		
尺寸	(1U)1.7(高)x 16.8(宽)x 17.0(深)英寸，适合标准的19英寸机架		
重量	17磅(7.7千克)		
运行环境	5°C–35°C		
非运行环境	0°C–50°C		
相对湿度	10%–90%(无结露)		
电源要求	115-230V，50/60 Hz – 750W		
法规核准	FCC Part 15 Class A CE Mark Class A EN 55032:2012、EN 55024:2010、 EN 61000-3-3:2013、EN 61000-3-2:2014		

Spirent CF20

适用于CyberFlood

系统要求

在运行CyberFlood时，访问虚拟主机/CyberFlood控制器的客户端最低要求如下:

- 运行最新浏览器版本(2017年6月或更新的版本)的任意Windows、Mac或Linux PC机
- Firefox浏览器
- Google Chrome浏览器

订购信息

由于可用系统配置的内容极其广泛，如果您需要详细的订购信息，敬请接洽您所在地区的思博伦销售代表。

思博伦服务

专业服务

- 测试实验室优化:测试自动化工程服务
- 服务部署和服务水平优化:厂商验收测试、SLA基准测试、基础设施和安全性验证
- 设备扩展能力优化:POC高扩展能力验证测试

教育服务

- 基于Web的培训:24 x 7硬件和软件培训
- 讲师带领的培训:亲身体验式方法和产品培训
- 认证:SCPA和SCPE认证

实施服务

- 经优化的新客户生产效率，包含最多三天的现场协助。

联系我们

欲了解更多信息，请致电思博伦销售代表或访问我们的网站www.spirent.cn/ContactSpirent。

北京代表处
地址：北京市东长安街1号东方广场东方经贸城W1座8层804-805A室
邮编：100738
电话：(86 10)8518 2539
传真：(86 10)8518 2540

思博伦通信（亚洲）有限公司
地址：香港北角英皇道243-255号国都广场19楼1905-07室
电话：(852)2511-3822
传真：(852)2511-3880

上海代表处
地址：上海市淮海中路283号香港广场3402室
邮编：200021
电话：(86 21)6390 7233 / 6070
传真：(86 21)6390 7096

技术支持热线：400-810-9529
中文网站：www.spirent.cn
全球网站：www.spirent.com

广州代表处
地址：广州市环市东路403号广州国际电子大厦2002室
邮编：510095
电话：(86 20)8732 4026 / 4308
传真：(86 20)8732 4120

技术支持网站：support.spirentcom.com
全球服务网站：www.spirent.com/GS
思博伦网络测试学院：www.spirentcampus.cn

思博伦通信科技（北京）有限公司
地址：北京市海淀区学院路35号世宁大厦13层
邮编：100191
电话：(86 10)8233 0055
传真：(86 10)8233 0022

© 思博伦通信公司2020年版权所有。文档中涉及的所有公司名称和/或商标名称和/或产品名称，特别是名字Spirent和带有标识的设备均是依据相关国家法律已经注册的商标或正在办理注册的商标。所有权利受到保护，如有变化不另行通知。 Rev. A CN 202006